Binary Sequences with Merit Factor > 6.3

Raymond A. Kristiansen and Matthew G. Parker

Abstract— **A method is described for the construction of binary sequences of very long length and with asymptotic Merit Factor > 6.3. The result is backed up by strong experimental evidence although no formal proof for the asymptote is known. The sequences were found by Kristiansen [1] using a small deterministic search, which we describe. Borwein, Choi and Jedwab [2] have independently identified a Merit Factor asymptote of 6.3421.... After we became aware of their work we realised that the sequences we construct are more simply described as periodic extensions of periodically-rotated Legendre sequences.**

Keywords— **Aperiodic Autocorrelation, L4 Norm, Legendre Sequence, Merit Factor, Quadratic Residue Sequence.**

I. Introduction

Binary sequences with high *Merit Factor* are desirable objects, having uses in telecommunications, information theory, physics, and chemistry. However they are also very difficult to find and/or construct, in particular as sequence length increases. The Merit Factor metric was first proposed by Golay [3], [4] as a way to measure sequences with low aperiodic autocorrelation sidelobes. Høholdt [5] proved that the Merit Factor of a random binary sequence approaches 1.0 as sequence length increases. The highest Merit Factor known is 14.08 and is satisfied by a length 13 binary Barker sequence. Barker sequences are binary sequences with aperiodic autocorrelation coefficients, $a_k \in \{-1, 0, 1\}, \forall\ k \neq 0$. It is conjectured that Barker sequences exist only when N is prime and $N \leq 13$, and Storer and Turyn [6] proved this Barker conjecture for all odd N.

An exhaustive search of binary sequences of length N examines 2^N sequences with $O(N^2)$ operations for each inherent Merit Factor computation. Turyn (see Golay [7]) and Lindner [8] did exhaustive searches up to length 32, and length 40, respectively. Mertens [9], [10] has searched exhaustively up to length 58 using a branch and bound algorithm of complexity $O(1.85^N)$, and has estimated that the maximal Merit Factor for a large length sequence will be > 9.0.

Partial search strategies have found binary sequences with high Merit Factor for higher lengths N. Based on the observation that all odd Barker sequences are skewsymmetric, Golay found sequences with relatively high Merit Factor by using a sieve to limit the search to skewsymmetric sequences up to length 59 [4] and later [11] length 117. Golay searched for symmetric and antisymmetric sequences with Merit Factor > 1.0, and found many sequences with Merit Factor > 8, and even some with Merit Factor > 9. Militzer et al [12] describe an evolutionary search for skewsymmetric binary sequences, finding sequences of length up to 201 with Merit Factor > 7.

Currently, for $N > 200$, computer search techniques are infeasible and one becomes reliant on construction techniques to obtain binary sequences with high Merit Factors. In this paper we are interested in high Merit Factor constructions for selected values N, as $N \to \infty$. Turyn established that a Legendre sequence of length N, N prime, periodically-rotated by $\frac{N}{4}$, has a Merit Factor that asymptotes to 6.0 as $N \to \infty$ (see Golay [13]). It was similarly found by Jensen, Jensen and Høholdt [14] that the Merit Factor of Modified Jacobi sequences of length $N = pq$, periodically-rotated by $\frac{N}{4}$, similarly asymptote to 6.0 as $N \to \infty$, given certain conditions on p and q. Parker [15] has presented a negaperiodic construction for binary sequences of length $N = 2p$, p prime, whose Merit Factor also appears to asymptote to 6.0 as $N \to \infty$, but this time the sequence is not rotated first. Høholdt and Jensen [16] conjectured that no infinite construction will be found that achieves an asymptotic Merit Factor higher than 6.0 and that, therefore, the rotated Legendre sequences are optimal. Since this conjecture was put forward, and in response to its implied challenge, various researchers have attempted to disprove the conjecture by devising constructions for binary sequences with asymptotic Merit Factor > 6.0, but to no avail, and it has become a source of much debate as to whether such sequences can be constructed. Recently Kirilusha and Narayanaswamy

This work was supported by the Norwegian Research Council.

Kristiansen and Parker are both with the Selmer Centre, Inst. for Informatikk, Høyteknologisenteret i Bergen, University of Bergen, Bergen 5020, Norway. E-mail: `raymond@ii.uib.no,matthew@ii.uib.no`. Web: `http://www.ii.uib.no/~matthew/`

[17], two students of Jim Davis, presented numerical evidence up to length ≈ 3000 (including Merit Factors greater than 6.2) that a Legendre sequence of length $p = 4k+3$, periodically rotated, then periodically extended by p^a, might, after all, satisfy an asymptotic Merit Factor strictly greater than 6, although no asymptote was uncovered. Kristiansen [1] and, independently, Borwein, Choi, and Jedwab [2], both inspired by Kirilusha and Narayanaswamy, have subsequently identified an asymptote, valid for Legendre sequences of any prime length, with the optimal rotation as $\approx cp$ and the subsequent extension as $\approx dp$, for c and d constants, although the periodic nature of this rotation and extension only became clear to us after reading the preprint [2]. Kristiansen [1] presented numerical evidence (up to length 20000) to obtain the rough figures of $c \le 0.25$ and $d \approx 0.059$, and [2] presented numerical evidence (up to length 4000000) and further provided highly-convincing theoretical arguments, that depend on a conjecture regarding truncated rotated Legendre sequences, for the values to be $c = 0.2211\ldots$ (and also $c = 0.7211\ldots$) and $d = 0.0578\ldots$. [1] conjectures an asymptote of > 6.3, and [2] gives theoretical reasoning for the asymptote to be $6.3421\ldots$. However, it is clear that the essential form of the construction, namely as a periodic extension of a periodically rotated Legendre sequence, is due to Kirilusha and Narayanaswamy [17], under the guidance of their supervisor, Jim Davis.

In the sequel we describe how we constructed these sequences with conjectured asymptotic Merit Factor > 6.3. The result was submitted as part of Kristiansen's Master's thesis [1]. We rely on a relatively low-complexity deterministic search. This search was later found to be not strictly necessary [2], but we observe that, as $N \to \infty$, the search periodically extends the Legendre sequence of length N to length $\frac{3}{2}N$, which is an interesting result in its own right.

II. Definitions

The *Aperiodic Autocorrelation Function* (AACF) of a binary sequence, $\mathbf{s}$, is defined as

$$\mathrm{AACF}_k(\mathbf{s}) : a_k = \sum_{i=0}^{N-k-1} (-1)^{s_i - s_{i+k}}, \qquad 1 \le k < N \tag{1}$$

The Golay *Merit Factor* (MF) of a binary sequence $\mathbf{s}$ of length N is given by [4]

$$\mathrm{MF}(\mathbf{s}) = \frac{N^2}{2\sum_{k=1}^{N-1} |a_k|^2}. \tag{2}$$

The optimal (highest) Merit Factor for a binary sequence $\mathbf{s}$ of odd length N is obtained when the AACF values are of the form $a_k = \{N, 0, \pm1, ..., \pm1, 0, \pm1\}$, and for N even, $a_k = \{N, \pm1, 0, \pm1, ..., \pm1, 0, \pm1\}$. This translates to a very loose upper bound on the aperiodic Merit Factor of a binary length N sequence of $\frac{N^2}{N-1}$ or N for N odd or even respectively.

Let $\mathcal{C}$ be a class of sequences, and let $\mathbf{s_N} \in \mathcal{C}$ be a sequence of length N. The *asymptotic Merit Factor* for the class $\mathcal{C}$ is

$$\lim_{N\to\infty} \mathrm{MF}(\mathbf{s_N}) = \mathcal{F}_{\mathcal{C}}. \tag{3}$$

The *sum-of-squares*, σ, of $\mathbf{s}$, is given by

$$\sigma(\mathbf{s}) = \sum_{k=1}^{N-1} |a_k|^2. \tag{4}$$

The Merit Factor can now be written as

$$\mathrm{MF}(\mathbf{s}) = \frac{N^2}{2\sigma}. \tag{5}$$

A Legendre sequence can be constructed from a Hadamard difference set [14]. The class of Legendre sequences periodically rotated by $\frac{1}{4}$ have an asymptotic Merit Factor of 6.0 [13], [16] and is one of only a few classes that have this highest known asymptotic Merit Factor.

The construction of a Legendre sequence of length $N = p$, p prime, can be achieved by finding a subset $\mathcal{S}$ of Z_p which specifies the positions of the 1s in the characteristic sequence, $\mathbf{s}$, of $\mathcal{S}$:

$$s_t = \begin{cases} 1 & \text{if } t \in \mathcal{S} \\ 0 & \text{if } t \notin \mathcal{S} \end{cases}, \tag{6}$$

when $0 \le t \le p-1$. The subset $\mathcal{S}$ is generated using a primitive generator α of $\mathrm{GF}(p)$,

$$\mathcal{S} = \left\{ \alpha^{2i} \bmod p \quad | \quad i = 0, ..., (\frac{p-1}{2}) - 1 \right\} \tag{7}$$

Let $\mathbf{s}'$ be a *periodic rotation* by u of a length N sequence, $\mathbf{s}$. Then $s'_i = s_{i-u \bmod N}$, $0 \le i < N$. Golay [13] showed that a length N Legendre sequence, periodically rotated by u, has an asymptotic Merit Factor $\mathcal{F}$ such that

$$\frac{1}{\mathcal{F}} = (\frac{2}{3} - 4|\frac{u}{N}| + 8(\frac{u}{N})^2), \quad |u| \le \frac{N}{2} \tag{8}$$

Høholdt and Jensen [16] rigourously proved this result and conjectured that, for a given binary construction, the maximum asymptotic value of the Merit Factor is 6.0 and, therefore, that the rotated Legendre sequences are asymptotically optimal.

Let $\mathbf{s}'$ be a *negaperiodic rotation* by u of a length N sequence, $\mathbf{s}$. Then $s'_i = \overline{s_{i-u \bmod N}}$, $0 \leq i < u$, and $s'_i = s_{i-u \bmod N}$, $u \leq i < N$, where '$\overline{*}$' means binary complement of $*$. Given a sequence, $\mathbf{s}$, of length N, then a *periodic extension* of $\mathbf{s}$ by l is the length $N+l$ sequence, $\mathbf{s}'$, such that,

$$s'_i = s'_{(i \bmod N)}, \qquad 0 \leq i < N+l$$

III. The Construction

Our construction has two stages:

- Directed Search: From an initial length N starting sequence, $\mathbf{s}$, execute a binary tree search with Merit Factor of the current sequence as the decision metric. After a pre-determined number of steps, l, output a length $N+l$ sequence $\mathcal{T}$, where $\mathcal{T} = \mathbf{s}|\mathbf{e}$, is a concatenation of the initial sequence, $\mathbf{s}$, with a length l extension, $\mathbf{e}$.
- Extended Directed Search: Look for a subsequence, $\mathbf{b}$, of length $N' = N+d$ within $\mathcal{T}$ which has highest Merit Factor. Output $\mathbf{b}$.

We now describe these two stages in more detail.

A. Directed Search

Choose an initial binary sequence, $\mathbf{s_0}$, of length N. At each step of the search there are two new possible sequences of length N, these being either the periodic or negaperiodic rotation of $\mathbf{s_0}$ by 1 position. Let $\mathbf{s_i^0}$ and $\mathbf{s_i^1}$ be the periodic and negaperiodic rotations of $\mathbf{s_{i-1}}$ by 1 position, respectively. At step i we assign $\mathbf{s_i} = \mathbf{s_i^0}$ or $\mathbf{s_i} = \mathbf{s_i^1}$, depending on which of $\mathbf{s_i^0}$ and $\mathbf{s_i^1}$ has the highest Merit Factor. The Directed Search then implements the following:

Decision Rule: Let $\mathbf{s_{i-1}}$ be a binary sequence of length N. Then,

$$\mathbf{s_i} = \begin{cases} \mathbf{s_i^1} & \text{if } \mathrm{MF}(\mathbf{s_i^1}) > \ \mathrm{MF}(\mathbf{s_i^0}) \\ \mathbf{s_i^0} & \text{otherwise} \end{cases} \tag{9}$$

(9) is slightly arbitrary in that, if there is a metric 'collision', i.e. when $\mathrm{MF}(\mathbf{s_i^0}) = \mathrm{MF}(\mathbf{s_i^1})$, then we choose the next sequence in the search as $\mathbf{s_i^0}$. We refer to this choice as Decision A. If instead we had chosen $\mathbf{s_i^1}$ then that would be Decision B. It turns out that when our starting sequence, $\mathbf{s_0}$, is a Legendre sequence then what we do when we have a metric collision is not so important, asymptotically.

Let x_i be the least significant bit of $\mathbf{s_i}$ (i.e. the single bit where $\mathbf{s_i^0}$ and $\mathbf{s_i^1}$ differ). We can use the Directed Search to *extend* the initial sequence, $\mathbf{s_0}$, by the successive bits, x_i so that, after l applications of (9), we have extended the length N sequence, $\mathbf{s_0}$, to the length $N+l$ sequence $\mathcal{T} = \mathbf{s_0}|\mathbf{e} = \mathbf{s_0}|x_1|x_2|\ldots|x_l$, and this is the sequence we output from the first stage of the construction.

An important aspect of the Directed Search is that each step only requires an *update* of the current autocorrelation values, therefore reducing the complexity of each Merit Factor computation from $O(N^2)$ to $O(N)$. Let $a_k(\mathbf{s_i})$ be the kth aperiodic autocorrelation coefficient for a binary sequence $\mathbf{s_i}$ of length N. Let $s_{i,j}$ be the jth element of the sequence, $\mathbf{s_i}$. Then one can show that,

$$\begin{aligned} & a_k(\mathbf{s_{i+1}}) \\ & \quad = a_k(\mathbf{s_i}) - s_{i,N-1}(s_{i,N-k-1} - s_{i,k-1}), \quad \mathbf{s_{i+1}} = \mathbf{s_i^0} \\ & \quad = a_k(\mathbf{s_i}) - s_{i,N-1}(s_{i,N-k-1} + s_{i,k-1}), \quad \mathbf{s_{i+1}} = \mathbf{s_i^1} \end{aligned} \tag{10}$$

For a Directed Search through l sequences, where l is a linear function of N, the search complexity is thus reduced from $\mathrm{O}(N^3)$ to $\mathrm{O}(N^2)$.

Example 1: Let $N = 7$ and let our initial sequence be $\mathbf{s_0} = 0110101$. The Merit Factor of this sequence is 1.0652. The Merit Factors of $\mathbf{s_1^0} = 1101010$ and $\mathbf{s_1^1} = 1101011$ are computed as 0.7903 and 2.2273, respectively, so we choose $\mathbf{s_1} = \mathbf{s_1^1} = 1101011$, as $2.2273 > 0.7903$. For the second step, the Merit Factors of $\mathbf{s_2^0} = 1010110$ and $\mathbf{s_2^1} = 1010111$ are 1.0652 and 1.2895, respectively, so we choose $\mathbf{s_2} = \mathbf{s_2^1} = 1010111$. Let $l = 6$. Then, after 6 steps the sequences $\mathbf{s_i}$ are:

$$0110101, 1101011, 1010111, 0101111, 1011110, 0111101$$

Therefore $\mathcal{T} = \mathbf{s_0}|\mathbf{e} = 0110101|11101$.

□

B. Extended Directed Search

We now test the Merit Factor of all length N' subsequences of $\mathcal{T}$ in order to find the subsequence with the highest Merit Factor, where $N' = N+d$, $0 \leq d \leq l$. The intuition behind this search is that, as the length N' subsequence comprises $d+1$ subsequences of length N each with relatively high Merit Factor, then the length N' subsequence, itself, should also have high Merit Factor. The construction is visualised in Fig. 1. The sequence $\mathcal{T}$ is constructed from the starting sequence of length N, and the l new bits from the Directed Search. We calculate the Merit Factor for the $l-d-1$ different subsequences $\mathbf{b_k}$, $0 \leq k < l-d$ of length $N+d$. We then output the subsequence, $\mathbf{b_i}$,

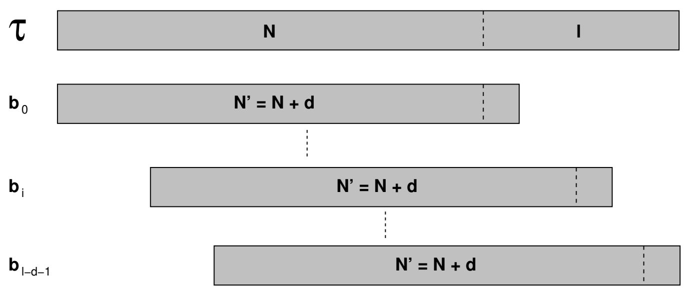

Fig. 1
Extended Directed Search

that satisfies

$$MF(\mathbf{b_i}) \geq MF(\mathbf{b_k}), \quad 0 \leq k < l - d$$

Example 2: Let the initial sequence, $\mathbf{s_0} = 0110101$. Perform the Directed Search $l = 21$ times to construct $\mathcal{T} = 0110101111010000101111010000$. Let $d = 1$. Then we compute the Merit Factor for subsequences $\mathbf{b_i}$ of length $N' = 8$, $\mathbf{b_i} \in \{01101011, 11010111, 10101111, ...\}$. It is found that $\mathbf{b_1} = 11010111$ has the highest Merit Factor $= 2.6667$.

□

C. The Legendre Extended Directed Search

We tried a number of starting sequences, $\mathbf{s_0}$, for the Extended Directed Search, but the (unrotated) Legendre sequence appeared to be the best choice. For $\mathbf{s_0}$ a Legendre sequence, experimental results [1] led us to identify the following optimal value for d (d_{opt}) and minimum value for l (l_{min}), such that a subsequence of length $N + d_{opt}$ and optimal Merit Factor can be found within the sequence $\mathcal{T}$ of length $N + l_{min}$.

$$d_{opt} = d(N) \approx 0.059N + 0.77 \tag{11}$$

$$l_{min} = l(N) \approx 0.31N + 20 \tag{12}$$

Using (11) and (12), an Extended Directed Search for all prime N, $100 \leq N \leq 20000$ was undertaken, using the Legendre sequence as a starting sequence, and the results are shown in Fig. 2, showing a clear Merit Factor asymptote of $6.34\ldots$.

Based on the experimental data a conjecture is proposed :

Conjecture 1: Let $\mathcal{T}$ be a binary sequence of length $N + l$, N prime, $l = 0.31N + 20$, let $\mathcal{T}_i$ be the ith element of $\mathcal{T}$, and let the first N bits of $\mathcal{T}$ be the

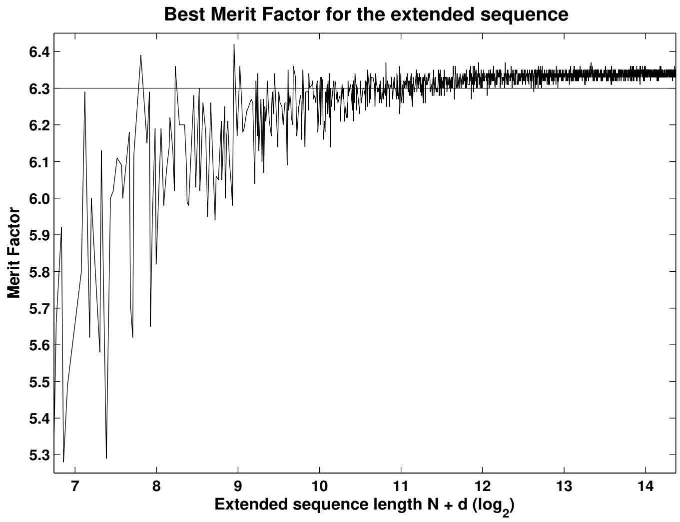

Fig. 2
Legendre Extended Directed Search with $d_{opt} = 0.059N + 0.77$ and $l = 0.31N + 20$, $101 \leq N \leq 19997$

Legendre sequence of length N. The last l bits of $\mathcal{T}$ are then found by

$$\mathcal{T}_{N+k-1} = \begin{cases} 1 & \text{if } \mathrm{MF}(\mathcal{T}_k, \mathcal{T}_{k+1}, ..., \mathcal{T}_{N+k-2}, 1) \\ & \qquad > \mathrm{MF}(\mathcal{T}_k, \mathcal{T}_{k+1}, ..., \mathcal{T}_{N+k-2}, 0) \\ 0 & \text{otherwise} \end{cases}$$

for $1 \leq k \leq l$. Then there exists a subsequence of length $N+d$, $d = \lfloor 0.059p + 0.77 \rfloor$, inside the sequence, $\mathcal{T}$, with Merit Factor > 6.3 for any large N.

To search for subsequences, $\mathbf{b'}$, of $\mathcal{T}$, of length N, observe that the aperiodic autocorrelation coefficients, $a_k(\mathbf{b'})$, are easily computed from $a_k(\mathbf{b})$, if $\mathbf{b}$ is of length $N - 1$, with complexity O(1),

$$a_k(\mathbf{b'}) = a_k(\mathbf{b}) + b'_{N-1}b'_{N-k} \tag{13}$$

Using (10), the complexity of a Directed Search through l sequences of length N can be reduced to $\mathrm{O}(l \cdot N + N^2)$. If l is a constant or a linear function of N this becomes $\mathrm{O}(N^2)$. For the Extended Directed Search, using (10) and (13), the complexity of computing successive Merit Factors of subsequences of length $N' = N + d$ will be $\mathrm{O}(d \cdot N)$ for the first subsequence, and $\mathrm{O}(l \cdot N)$ for subsequent subsequences. So overall, as d and l are linear functions of N, the complexity of the Extended Directed Search is still $\mathrm{O}(N^2)$, the same as for the Directed Search for a single length sequence. Therefore the complexity to find the sequence with Merit Factor > 6.3, as described in Conjecture 1, is $\mathrm{O}(N^2)$. This complexity analysis was confirmed experimentally [1].

IV. Periodic Extension via Directed Search

The Extended Directed Search of Section III-B assumes that the l extension bits bear no obvious relationship to the first N bits. However it turns out that if the starting sequence is a Legendre sequence then the Directed Search *periodically extends* the sequence. We realised this only after reading the preprint by Borwein, Choi and Jedwab [2]. Let us take $l = (0.2211 + 0.0578) \cdot N = 0.2789 \cdot N$ which, according to computations by Borwein, Choi and Jedwab, is an accurate estimate of the periodic extension of the length N Legendre sequence such that the length $1.0578 \cdot N$ sequence starting at bit position $0.2211 \cdot N$ has an asymptotic Merit Factor > 6.34. Then we find, computationally, that there are only a few small N exceptions for which the extension as computed using the Directed Search is not a periodic extension of at least length l. These exceptions are for $N = 5, 7, 13, 37$. Furthermore, if we apply the Directed Search to the Legendre sequence for l' extension bits, where $l' \simeq 0.5 \cdot N$, and $N \to \infty$, then we still obtain a periodic extension. We arrive at the following conjecture,

Conjecture 2: For $\mathcal{T}$ constructed according to Conjecture 1, but with l replaced by l', then,

$$\mathcal{T}_k = \mathcal{T}_{N+k}, \quad 0 \leq k \leq l', \text{ where } l' \simeq 0.5 \cdot N \text{ as } N \to \infty. \tag{14}$$

The paper by Borwein, Choi, and Jedwab [2], using theoretical arguments, concludes that the asymptote of $6.3421\ldots$ is obtained if the Legendre sequence is first periodically rotated by about $0.2211 \cdot N$ (or $0.7211 \cdot N$) and then periodically extended by $0.0578 \cdot N$. Their figure of 0.0578 is in broad agreement with our figure of 0.059 for the optimal sequence extension length (see Conjecture 1). Moreover, although we did not try to identify a precise position for the optimal subsequence within $\mathcal{T}$, our rough figure of $0.31 - 0.059 = 0.251$ is quite close to 0.2211, and re-checking our results shows that the optimal subsequence within $\mathcal{T}$ starts at the ith bit of $\mathcal{T}$, where $i \simeq 0.22 \cdot N$ as $N \to \infty$. What is particularly surprising is that one would not expect our search technique to exactly regenerate bits of a Legendre sequence. We have no proof as to why it does. Fig. 3 shows the maximum possible length of the periodic extension of the Legendre sequence, generated by Directed Search, as a ratio $\frac{N+l'}{N}$ as $N \to \infty$. It is evident that $l' \simeq 0.5 \cdot N$ as $N \to \infty$. A complete search of all primes p up to $N = p = 19997$ identified six unusual primes where $l' > 0.5$, all of the form $N = 4k + 3$. Specifically, for $N = 3, 11, 31, 71$ the Directed Search periodically extends the Legendre sequence indefinitely. Moreover, for $N = 131, 751$ the Directed Search periodically extends up to length $131 + 130 = 261$, and $751 + 734 = 1485$, respectively, i.e. the Legendre sequence is <u>almost</u> completely repeated once. (In Fig. 3, the values for $N = 3, 11, 31, 71$ should be ∞ but, so as to include them on the graph we have (incorrectly) marked them with sequence length 2.0). Finally we found, computationally, that our search also periodically extends to length $\approx 1.5 \cdot N$ a length N Legendre sequence that has first been periodically rotated by $\lceil \frac{N}{2} \rceil$, as $N \to \infty$.

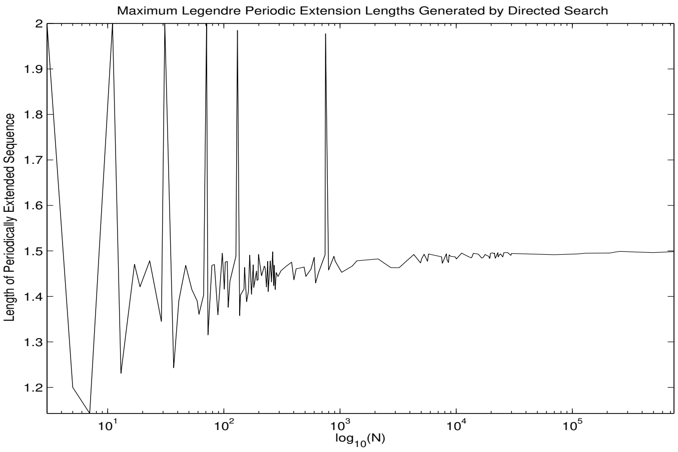

Fig. 3
Maximum Legendre Periodic Extension Lengths Generated by Directed Search

A. Decision B

From the Decision Rule of (9), we specify the following two metric collision strategies:

- **Decision A**: If $\mathrm{MF}(\mathbf{s_i^0}) = \mathrm{MF}(\mathbf{s_i^1})$, then choose $\mathbf{s_i^0}$.
- **Decision B**: If $\mathrm{MF}(\mathbf{s_i^0}) = \mathrm{MF}(\mathbf{s_i^1})$, then choose $\mathbf{s_i^1}$.

The Directed Search, as specified in (9) and Conjecture 1, uses Decision A. Computations indicate that metric collisions <u>never</u> occur when the starting Legendre sequence length is $N = p = 4k + 3$ so, in this case, Decision A generates the same sequence as Decision B. But, for $N = p = 4k + 1$, a metric collision <u>always</u> occurs on the first extension bit. However, if we use Decision B then apart from this first bit, the

Legendre sequence is periodically extended as before. As $N \to \infty$ then, once again, $l' \simeq 0.5$, the highest Merit Factor subsequence of $\mathcal{T}$ as $N \to \infty$ still has Merit Factor $\simeq 6.34$, is still of length $N + (0.059 \cdot N)$, and still starts at the ith bit of $\mathcal{T}$, where $i \simeq 0.22 \cdot N$. This follows for length $N = 4k + 1$ sequences generated using Decision B because they are simply those generated using Decision A with their first bit flipped.

V. Conclusion

We presented a construction for long-length binary sequences which appear to achieve an asymptotic Merit Factor of around 6.34. The results are experimental and it remains to find a proof for this Merit Factor asymptote. Independent work by Borwein, Choi, and Jedwab [2] has identified that these sequences are simply periodic extensions of periodically rotated Legendre sequences and, therefore, that there is no need for the search described here. However the search may have more general application, and it is also surprising that it is able to periodically extend a length N Legendre sequence up to length $\simeq 1.5 \cdot N$ as $N \to \infty$. Moreover, for prime lengths $N = 3, 11, 31, 71$, the periodic extension is infinite. It would be interesting to investigate the action of this search on other cyclotomically-generated sequences. Finally a new challenge is to find a construction for a family of binary sequences with asymptotic Merit Factor noticeably greater than 6.34.

References

[1] R.A. Kristiansen, "On the Aperiodic Autocorrelation of Binary Sequences", Master's Thesis, Selmer Centre, University of Bergen, Norway, - Submitted on March 7, 2003, http://www.ii.uib.no/~matthew/Masters/notes.ps.

[2] P. Borwein,K-K.S. Choi and J. Jedwab, "Binary Sequences with Merit Factor Greater than 6.34", *IEEE Trans. Inform. Theory - to appear in this issue*, 2004.

[3] M.J.E. Golay, "A Class of Finite Binary Sequences with Alternate Autocorrelation Values Equal to Zero", *IEEE Trans. Inform. Theory*, **18**, No 3, pp 449–450, May 1972.

[4] M.J.E. Golay, "Sieves for Low Autocorrelation Binary Sequences", *IEEE Trans. Inform. Theory*, **23**, No 1, pp 43–51, Jan 1977.

[5] T. Høholdt, "The Merit Factor of Binary Sequences", **Difference Sets, Sequences and their Correlation Properties, A.Pott et a. (eds.), Series C: Mathematical and Physical Sciences**, Kluwer Academic Publishers, **542**, pp 227–237, 1999.

[6] J. Storer and R.J. Turyn, "On Binary Sequences" *Proc. American Math. Soc.*, **12**, pp 394–399, 1961.

[7] M.J.E. Golay, "The merit factor of long low autocorrelation binary sequences", *IEEE Trans. Inform. Theory*, **28**, No 3, pp 543–549, May 1982.

[8] J. Lindner, "Binary sequences up to length 40 with best possible autocorrelation function", *Electronics Letters*, **2**, pp. 507, 1975.

[9] S. Mertens, "Exhaustive search for low-autocorrelation binary sequences", *J. Phys. A*, **29**, pp L473–L481, 1996.

[10] S. Mertens, "The Bernasconi model", http://odysseus.nat.uni-magdeburg.de/~mertens/bernasconi/, Accessed 2002.

[11] M.J.E. Golay, "A New Search for Skewsymmetric Binary Sequences with Optimal Merit Factors", *IEEE Trans. Inform. Theory*, **36**, No 5, pp 1163–1166, Sept 1990.

[12] B. Militzer, M. Zamparelli and D. Beule, "Evolutionary Search for Low Autocorrelated Binary sequence", *IEEE Trans. on Evolutionary Computation*, **2**, No 1, pp 34–39, Apr 1998.

[13] M.J.E. Golay, "The Merit Factor of Legendre sequences", *IEEE Trans. Inform. Theory*, **29**, No 6, pp 934–936, Nov 1983.

[14] J. Jensen, H. Jensen and T. Høholdt, "The Merit Factor of Binary Sequences Related to Difference Sets", *IEEE Trans. Inform. Theory*, **37**, No 3, pp 617–626, Jan 1991.

[15] M.G. Parker, "Even Length Binary Sequence Families with Low Negaperiodic Autocorrelation" *AAECC-14 Proceedings, Nov 26–30, Melbourne, Australia, Lecture Notes in Computer Science, LNCS 2227, Springer-Verlag*, pp 200–210 , Nov 2001.

[16] T. Høholdt and H. Jensen, "Determination of the Merit Factor of Legendre Sequences", *IEEE Trans. Inform. Theory*, **34**, No 1, pp 161–164, Jan 1988.

[17] A. Kirilusha and G. Narayanaswamy, "Construction of New Asymptotic Classes of binary sequences based on existing asymptotic classes", Dept. Math. and Comput. Science, Univ. of Richmond, Technical Report, http://www.mathcs.richmond.edu/~jad/summerwork/, 1999.

Biography - Matthew G. Parker

Matthew G. Parker obtained a B.Sc. from U.M.I.S.T., UK, in 1982 and a Ph.D. in VLSI and Number Theory from University of Huddersfield, U.K., in 1995. From 1995 - 1998 he worked as a postdoctoral researcher at University of Bradford, researching into OFDM and PAPR-related problems. From 1998 onwards he has been a researcher at the Selmer Centre, University of Bergen, Norway, researching into cryptography, quantum information theory, telecommunications and coding theory.

Biography - Raymond A. Kristiansen

Raymond A. Kristiansen obtained his degree and a Master's degree in 2003 from Institute for Informatics, University of Bergen, Norway, and is currently working in industry.